Inala et al. (U.S. Patent No. 6,199,077, hereinafter *Inala*). Office Action at ¶3. Applicants respectfully traverse these rejections as follows.

First, Applicants are unclear as to the basis for the Examiner's use of *Steinberger* and/or *Inala* as a reference against the present application. Applicants believe that the Examiner has not established that either of *Steinberger* or *Inala* qualify as prior art against the present application. If the Examiner maintains the present rejections in light of the further remarks below, Applicants request that the Examiner clarify his position in this regard.

Next, assuming only for the purpose of this analysis that these references constitute prior art, Applicants assert that the claimed invention is patentable over the combination of references cited. Turning to the Examiners rejection of claims 1 and 4-15 as unpatentable over *Takagi* in view of *Steinberger*. *Takagi* discloses an "information processing system in which the necessary information can be transferred via a network by the time this information becomes actually necessary, without damaging the utility and convenience from the user's point of view..." *Takagi* at 4:28-32. *Takagi* provides for provision of information based upon user-centric information for a specific end user (*e.g.*, end user schedule, type of information, etc.). *Id.* at 4:52-63; 5:9-20. *Steinberger* discloses "a system and method of using standards based procedures to collect historical top communicator information." *Steinberger* at 3:39-41. This system includes an RMON alarm/user history poller 28 connected to the SNMP stack 22. *Id.* at 6:14-16. "[I]f the top communicator information is located within the top communicator database 26, a check is performed to determine whether the time since the last update performed by the top communicator logic 100 is greater than the collection time interval specified by timer 32-1 (step 111). When the last updated time is greater than the collection time interval-1, a check is performed by the top communicator logic 100 as to whether the request for user data was an internal or external-call (step 112)." *Id.* at 6:18-26.

First, independent claims 1, 10 and 13 each include a limitation requiring determination of an update time for information stored by a selected information provider and the determination of an end user set based upon the determined update time. *Takagi* does not appear to disclose use of information provider centric information as a basis for determining information delivery. In the claimed invention, the expected update time for an information provider is first determined and then used as a basis for determining an end user update set. *Takagi* appears to be directed towards provision of static information to an end user; the system according to *Takagi* appears to determine what information is relevant and when it should be delivered. In contrast, the claimed invention deals with provision of information that is subject to periodic update under control of the information provider; the determined update time is used by the claimed invention to determine a set of end users whose information is potentially impacted by an update at the determined update time. In addition, *Takagi* appears does not appear to disclose identification of end user sets for update; rather, the *Takagi* appears to work on an individual end user basis.

Further, the claimed inventions require a sorting step based upon predicted login times for each end user in the determined set. *Takagi* appears to disclose a "prediction means" that may predict the login time for an individual user. *Takagi* at 3:57-67. *Takagi*, as discussed above however, does not appear to deal with sets of end user updates so the description the "prediction means" cited by the Examiner does not appear to perform any sorting of end users by predicted login times.

Next, the Examiner indicates that *Takagi* does not disclose the assignment of harvesting times to end users based upon the end user's predicted login time. The Examiner asserts that this limitation is disclosed by *Steinberger* - "User history poller act as harvesting time for each end-user, It collects the information on user and perform a check on user's history. Check can be predicting user's login time." [*sic*] Office Action at ¶2. Applicants respectfully assert that the history poller does not appear to assign harvest times to each end user but rather to collect aggregated communicator data at

periodic intervals. Further, the Examiner states that the check "can be" predicting user's login time. Applicants would respectfully request that the Examiner provide a citation in *Steinberger* for this assertion.

For at least the reasons above, Applicants believe that claim 1, 10 and 13 are allowable over *Takagi* in view of *Steinberger*. As claims 2-9, 11-12 and 14-15 depend directly or indirectly from claims 1, 10 and 13 respectively, these dependent claims also include the limitations discussed above with respect to claims 1, 10 and 13 and therefore, should similarly be allowable. Applicants respectfully request that the Examiner withdraw the rejection of these claims.

Applicants further assert that with respect to claim 5 the *Takagi-Steinberberger* combination does not teach or suggest the recited limitations of this claim. Specifically, Applicants assert that this combination fails to teach or suggest the recited steps for generating a predicted login time involving determining whether each end user's login time profile meets a predetermined confidence threshold and then assigning a predicted login time based upon that determination. Applicants assert that neither Steinberger nor Takagi appear to teach or suggest determining whether a login profile associated with an end user meets a predetermined confidence threshold. The passage of *Steinberger* cited by the Examiner does not appear to teach or suggest use of analysis of login profiles for a confidence level threshold test and generating a predicted login time based upon the test result; *Steinberger* does mention certain checks that are performed such as whether a certain time interval has elapsed or as whether a particular request was internal or an external-call but does not appear to discuss verifying a confidence level for a login profile against a threshold. *Steinberger* at 8:20-49. Since *Steinberger* does not appear to perform the test recited in the claim limitation, it cannot generate a predicted login time that corresponds to the present day and time where the confidence level threshold test fails or a predicted login time based upon the login profile where the confidence level threshold test is met. Similarly, the passage of *Takagi* cited by the Examiner does not appear to teach or suggest use of

analysis of login profiles for a confidence level threshold test and generating a predicted login time based upon the test result. The cited passage outlines use of a threshold test in one of its Habit Knowledge rules. *Takagi* at 15:59-16:8. The discussed threshold test evaluates remaining work on a project against an available work time (determined by subtracting the date and time of prediction from the deadline for the project). *Id.* This ratio is compared to one or more threshold values. *Id.* Applicants acknowledge that a threshold test is described in *Takagi*; however, Applicants assert that the threshold test in *Takagi* is not a confidence level threshold test performed on user login profiles and that the result of the threshold test in the cited passage of *Takagi* is not the generation of a predicted login time that is either the present day and time if the confidence level does not meet the threshold or a predicted login time based upon the login profile. For at least these additional reasons, Applicants respectfully request that the Examiner withdraw the rejection of this claim.

Applicants further assert that with respect to claim 8 the *Takagi-Steinberger* combination does not teach or suggest the recited limitations of this claim. Specifically, Applicants assert that this combination fails to teach or suggest the recited steps for assigning a harvesting time in the manner claimed.

According to this claim, the assignment of a harvest time occurs in the manner prescribed by the recited step limitations. One step in the claim requires performing a distribution fit across time to generate a polynomial function that allows determination of the number of end users subject to harvesting over a specified time period. The Examiner cites *Steinberger* at 8:50-9:11 as teaching this limitation. Applicants respectfully assert that the cited passage fails to teach or suggest this limitation. The cited passage describes manipulation of a host list and performance of calculations based thereon. *Id.* After host information is collected, a user provided exclusion inquiry is processed to determine if any identified host has not been inspected according to a user provided host exclusion algorithm. *Id.* at 8:54-62. Various calculations are performed on the listed hosts not subject to exclusion and the calculated results stored.

Id. at 9:2-11. This passage does not appear to discuss the generation of a polynomial function quantifying end users subject to harvesting over a given time period.

This claim further recites determining a network activity curve associated with the host computer and the selected information provider, generating an inverse of the determined network activity curve and performing an integral matching algorithm using the generated polynomial function and the generated inverse of the network activity curve. The Examiner cites *Takagi* at 27:5-64 as teaching these limitations. Applicants acknowledge that the cited passage discusses various types of statistical data calculations and correlations. *Takagi* discusses "correlation between the time/time zone and the work content" (*Id.* at 27:1-26), "correlation between the application and the data" (*Id.* at 27:27-44) and "correlation between the application and the place" (*Id.* at 27:45-64.). None of these correlations appears to deal with generating a graph or statistics related to network activity, manipulating (inverting) such a network activity graph or statistics or performing an integral matching algorithm using such a network activity graph or statistics and a generated polynomial function.

Applicants assert that *Takagi* and *Steinberger* alone or in combination fail to disclose the requisite steps recited in this claim for assigning a harvest time. For at least these additional reasons, Applicants respectfully request that the Examiner withdraw the rejection of this claim.

The Examiner has rejected claims 2 and 3 under 35 U.S.C. §103(a) as being obvious over *Takagi* in view of *Steinberger* in further view of *Inala*. Office Action at ¶3. The disclosures of *Takagi* and *Steinberger* are discussed above. *Inala* discloses "an Internet-connected server; and a portal software executing on the server, including a summary software agent. The Portal maintains a list of Internet destinations specific for a subscriber, and the summary software agent accesses the Internet destinations, retrieves information according to pre-programmed criteria, and summarizes the retrieved information for delivery to the subscriber." *Inala* at 2:60-67.

Claims 2 and 3 depend directly or indirectly from claim 1. Applicants assert that the arguments above with respect to the failure of the *Takagi-Steinberger* combination to teach or suggest the ascribed limitations of claim 1 apply with equal merit to the Examiners rejection of claims 2 and 3. Consequently, for at least the reasons discussed above with respect to claim 1, Applicants respectfully request that the Examiner withdraw the rejection of these claims.

In addition, claims 2 and 3 provide limitations prescribing a particular approach to determining a set of end users. The claim limitation require selection of end users configured to receive information from the selected information provider and the elimination from this group those end users not configured to receive information subject to the update at the determined update time. The Examiner support his assertion that *Inala* discloses these limitation by citation to a passage of *Inala* describing a user profile including URLs and username/password pairs and an interface for maintaining such user subscription; the user profile potentially defines a set of information providers for a single user. *Inala* at 5:50-65. The referenced passage does not appear to describe, teach or suggest a process for determining a set of end users potentially impacted by a particular update by a particular information provider that creates an initial set of end users configured to receive information from the particular provider then eliminating those not configured to receive information subject to the determined update. Applicants respectfully request that the Examiner withdraw the rejection of these claims for at least these additional reasons.

Conclusion

For at least the reasons stated above, the Applicants respectfully submit that each of the claims pending in the application is allowable, and therefore courteously solicit the allowance of the claims.

The Examiner is invited and encouraged to directly contact the undersigned if such contact may enhance the efficient prosecution of this application to issue.

A credit card payment authorization form PTO-2038 for $55.00 is enclosed, together with a Request for a one-month Extension of Time. No additional fee is believed to be due with this Amendment and Response to Office Action. If, however, the Commissioner believes that a fee is due, the Commissioner is hereby authorized to charge any such additional fee(s) from, or credit any fee overpayment(s) to, Deposit Account No. 14-0629.

Respectfully submitted,

NEEDLE & ROSENBERG, P.C.

David S. Kerven, Ph.D.
Registration No. 43,712

Certificate of Mailing

I hereby certify that this correspondence and any items indicated as attached or included are being deposited with the United States Postal Service in an envelope addressed to: Commissioner for Patents, Washington, D.C. 20231, on the date indicated below.

Lucy J. Lehman — 9/6/02

Lucy J. Lehman — Date

APPENDIX A
MARKED UP COPY OF THE SPECIFICATION

Please replace the paragraph at page 2, line 20 – page 3, line 15 with the following:

FIG. 1 displays the current process of acquiring online personal information (PI) 100. The end user first selects an information provider site in step 110. The end user proceeds to step 120 by locating and entering the Internet address of the selected information provider. This step may be accomplished in several manners with varying levels of complexity. A simple means for accomplishing this step is the utilization of a bookmark or favorite whereas locating an information provider for the first time might involve significant time and effort performing online searches. In step 130, the end users logs into the selected information provider's Web site utilizing the site's specific logon protocol. This protocol usually involves verifying the identity of the end user using a user name and password or other means of verification, acquiring the verification data from cookies residing on the end user's system or a combination of requested data and cookie data. The end user continues in step 140 by navigating through Web pages on the information provider's Web site until the desired information is located. During this process, the end user is often required to visit Web pages of little or no use to the end user whose goals is to simply acquire the particular PI residing on the Web site. Ultimately in step 150, the end user is presented with the desired PI. The entire process 100 is repeated for each individual piece of PI desired by the end user. Under this PI access model, the end user must visit each separate information provider, track potentially different identity verification data for each, utilize a different user interface at each site and possibly wade through a significant number of filler Web pages.

Please replace the paragraph on page 10, lines 14 - 23 with the following:

In addition, or as an alternative, the PI associated with each end user 210 may reside on his/her client computer 220 using cookie technology as specified in D. Kristol

and L. Montulli, "HTTP State Management Mechanism", Request For Comments (RFC) 2109, February, 1997 (available at http://www.ietf.org/rfc/rfc2109.txt), which is expressly incorporated herein in its entirety. The PI associated with the end user 210 would be stored as PI cookies 375. This implementation mechanism provides inherent support for segregating PI associated with one end user 375 from PI associated with all other end users. Utilizing this method as a substitute for a centralized store provides a layer of security against unauthorized access. As a further measure, PI data stored in cookies could be stored in an encrypted format.

Please replace the paragraphs at page 12, line 11 – page 15, line 16 with the following:

The four primary processing components access and manipulate the data in the three stores. The processing components may execute on a single processor, such as a file server computer system based on a Pentium class (MMX, PRO, II, III, etc.) central processing unit or an equivalent, or multiple processors. These four processing components are the Baseline configure component 320, the end user configure component 330, the PI access/transact component 340 and the PI delivery component 350 as seen in FIG. 3. The Baseline configure component 320 provides the interface by which new user selectable PI providers are added to the system. This component 320 might be implemented in a variety of ways including trial and error followed by manual entry of configuration information, semi-automated trial and error (automated location of Hypertext Markup Language (HTML) <FORM> elements, Javascript functions and Java applets) followed by manual entry of configuration information or, preferably, configuration by example (executing the protocol in a simulated Web client where the simulated Web client automatically generates a list of required data and a list of steps in the access process). These processes would be utilized at two levels: the first level being the set of data and steps required for general access to the particular PI provider and the second level being the set of additional data and steps required for

accessing each particular piece of PI on the PI provider's site. The baseline configuration component 320 may be triggered independently when a new PI provider is added to the system, or it might be triggered as a result of a failure of the PI access/transact component 340 potentially indicating a change in access requirements for the failed access. This latter warning would more likely result where the PI access/transact component 340 has made a comparison between requirements supplied by the Provider store 310, both general to the PI provider and specific to the PI or transaction, and the end user data supplied by the user store 360 after seeking end user verification via a request of the end user to confirm the previously entered required access data via the end user configure component 330 and found an inconsistency. When an inconsistency is determined, updates to the Provider store [320]310 are made to bring the Provider data into conformance with current access/transaction requirements.

The end user configure component 330 allows an end user to select and configure PI and transactions of interest to the specific user. This configuration information is maintained in the user store 360. When an end user initially subscribes to the system according to the present invention, the system allows the user to select the types and sources of PI and/or transactions desired. First, the system requests permission from the end user to act on his behalf to obtain any selected PI and to execute any authorized transactions. Next, the system provides the user with a list of known information suppliers and the types of PI supplied from and transactions supported by the particular PI provider from the Provider store [320]310. The system requests the verification data necessary for accessing each selected PI provider and the additional data required by the particular PIs and/or transactions desired from that PI provider. Assuming the end user is already a registered user with the selected PI provider or the particular PI provider does not require prior registration, the data supplied by the end user is placed in the user store 360.

One method of obtaining any cookie data would be for the end user to access each previously accessed PI utilizing the PI engine 240 as a proxy server. The PI engine 240 would pass the cookie data to the PI provider site with the appropriate Web page requests to obtain the PI or execute the transaction and with the end user's permission retain a copy of the cookie data in the [his]end user's record in the user store 360. An alternate means of obtaining the cookie data would be a direct upload of the cookie information from the end user's computer. In a preferred embodiment, no cookie data is necessary where a user is already registered with a provider. All that is necessary is the verification data for login.

If the end user does not have the requisite information because he is not a registered user of a selected PI provider, the user configure component 330 prompts the user for the information necessary to register the end user with the PI provider and performs the registration procedure required by the PI provider. A simulated Web client could perform this process automatically supplying the access data as required and sending any necessary cookie data. The manner in which such a simulated client registers the end user depends significantly upon the interaction method used on the PI provider Web site. If the Web site uses HTML forms and common gateway interface (CGI) applications, the end user configure component 330 can formulate a uniform resource locator (URL) to replicate the effect of actual form usage and submit this URL to the simulated Web client. The use of a URL to mimic an HTML form is equivalent to manually entering the data into the Web <FORM> element. See Kerven, Foust, Zakour, HTML 3.2 Plus How-To, Waite Group Press, 1997, pp. 559-569. If the Web site uses a mixture of HTML forms and Javascript functions, a simulated Web client with a modified Javascript interpreter could effectively register the user by following the end user registration process for the particular PI provider. The registration process to follow would be obtained from the record of the particular PI provider in the Provider store [320]310. The Javascript interpreter in the simulated Web client would follow this procedure and supply the data supplied by the end user. A similar process could be

used if the registration process on the PI provider Web site utilizes a Java applet. A Web client with a modified Java bytecode interpreter could effectively register the user by following the end user registration process stored for the particular PI provider in the Provider store [320]310. The bytecode interpreter would supply the data previously entered by the end user rather than requiring interactive input from the end user. If the PI provider Web site utilizes a combination of forms, scripts and applets, the individual procedures above could be used in combination to accomplish the desired registration.

Please replace the paragraph at page 17, lines 1 – 19 with the following:

A failed registration could result from several situations. First, the end user attempting to register with the PI provider does not qualify for registration; for example, an end user attempting to register with a bank with whom the end user does not maintain an account and where the bank only allows access to account holders. Next, the end user may have supplied improper or incorrect information. For example, a bank registration process might require a social security number, a password, a bank account number and the maiden name of the end user's mother; if the user entered an incorrect social security number, the registration process would fail. Finally, the PI provider may have altered the registration procedure for its Web site. In this situation, following the process supplied from the Provider store [320]310 would yield a failed registration. In the instance of any registration failure, the end user could be presented with the data initially supplied to the system for registration. The system could then ask the end user to double check the correctness of the information provided and to correct and resubmit the data if an error is found. A second failure resulting from the submission of identical requisite data might generate an error message presented to the end user stating that either the end user is ineligible to access the selected PI from the selected PI provider or that alteration by the PI provider may have caused an error in registration. This second failure could also trigger a warning suggesting the need to potentially reconfigure the record for the PI provider in the Provider store [320]310.

Please replace the paragraphs on page 18, lines 20 – page 20, line 14 with the following:

With reference to FIG. 3, the PI access/transact component 340 supports the update, acquisition and transaction functionality of the PI engine 240. The PI access/transact component 340 is responsible for accessing and storing user PI and executing transactions authorized by the end user. When access or update is needed for a selected end user, the PI access/transact component 340 combines information from the Provider store [320]310 and the user store 360 to update end user PI in the PI store 280. For each piece of PI requiring access or update, the PI access/transact component 340 looks up the access procedure and information needed for the particular PI in the Provider store [320]310. The verification and access data is found in the user store 360. The PI access/transact component 340 utilizes this information to connect to the PI provider's Web site across the Internet and to access the PI. Where multiple pieces of PI require updating or access, the accesses may occur in series or parallel.

Requested transactions would be similarly supported. For each transaction, the PI access/transact component 340 combines information from the Provider store [320]310 and the user store 360 to perform the requested transaction. The PI access/transact component 340 looks up the transaction procedure and information needed for the particular transaction in the Provider store [320]310. The verification and access data is found in the user store 360. The PI access/transact component 340 utilizes this information to perform the transaction across the Internet from the PI provider's Web site.

A simulated Web client could perform access or transaction processes automatically supplying access and verification data as necessary. The manner in which such a simulated client access PI or execute transactions depends significantly upon the interaction method used on the PI provider Web site. If the Web site uses

HTML forms and common gateway interface (CGI) applications, the PI access/transact component 340 can formulate a uniform resource locator (URL) to replicate the effect of actual form usage and submit this URL to the simulated Web client. The use of a URL to mimic an HTML form is equivalent to manually entering the data into the Web <FORM> element. See Kerven, Foust, Zakour, HTML 3.2 Plus How-To, Waite Group Press, 1997, pp. 559-569. If the Web site uses a mixture of HTML forms and Javascript functions, a simulated Web client with a modified Javascript interpreter could effectively access the PI or perform the transaction by following the PI access/transact process for the particular PI or transaction respectively. The access or transaction process to follow would be obtained from the record of the particular PI or transaction in the Provider store [320]310. The Javascript interpreter in the simulated Web client would follow this procedure and supply the data found in the user store 360. A similar process could be used if the PI provider Web site utilizes a Java applet. A Web client with a modified Java bytecode interpreter could effectively access PI or perform transactions by following process stored for the particular PI or transaction in the Provider store [320]310. The bytecode interpreter would supply the data from the user store 360 rather than requiring interactive input from the end user. If the PI provider Web site utilizes a combination of forms, scripts and applets, the individual procedures above could be used in combination to accomplish the desired access.

Please replace the paragraph at page 29, lines 7 – 15 with the following:

The end user must first identify the Provider 110. Next, the end user must locate the Provider's Web address 120. Then, the user [the]requests the Provider's login page 130. If the end user does not remember the requisite information, this information must be found, or the desired information will remain inaccessible via the Web. The end user then navigates the Provider's Web site 140. This often entails visiting the Provider's main page 710 followed by viewing a variety of intermediate pages on the Provider's site 720. The end user may have to backtrack several times to the main

page 710 or accidentally leave the system entirely forcing a second login [140]130 before finally locating the desired information 150.

Please replace the paragraph at page 32, lines 12 – 21 with the following:

For instance, with reference to FIG. 2 an end user 210 would be able to maintain his/her accounts online through the PI Engine 240. If an information provider has the capability of receiving payments online, the PI Engine 240 could support complete or partial automation of such transactions. If there is a billing due date for a certain information provider, PI Engine 240 could flag that information and send email to the end user 210 notifying him/her of the bill due. Thus, the user will not have to check each of his/her providers individually for due date information. The PI Engine 240 could also automated payments on a limited range of billing amount for providers who allow payments over their Web servers [260]250, then send an email to the user with the notification of payment.

APPENDIX B
MARKED UP COPY OF THE CLAIMS

Please amend the indicated claims as follows:

11. (Amended) The system of claim 10, wherein the host computer processor performs the further step of harvesting the [personal] information for each end user in the determined set of end user from the selected information provider at the harvesting time assigned to each end user.

14. (Amended) The storage device of claim 13, and storing further instructions that upon execution cause the processor to perform the step of harvesting the [personal] information for each end user in the determined set of end user from the selected information provider at the harvesting time assigned to each end user.